Samarbejde bygget på forskellighed

Anbefalinger til offentlig-privat samarbejde om IKT-sikkerhed

Christensen, Kristoffer Kjærgaard; Petersen, Karen Lund

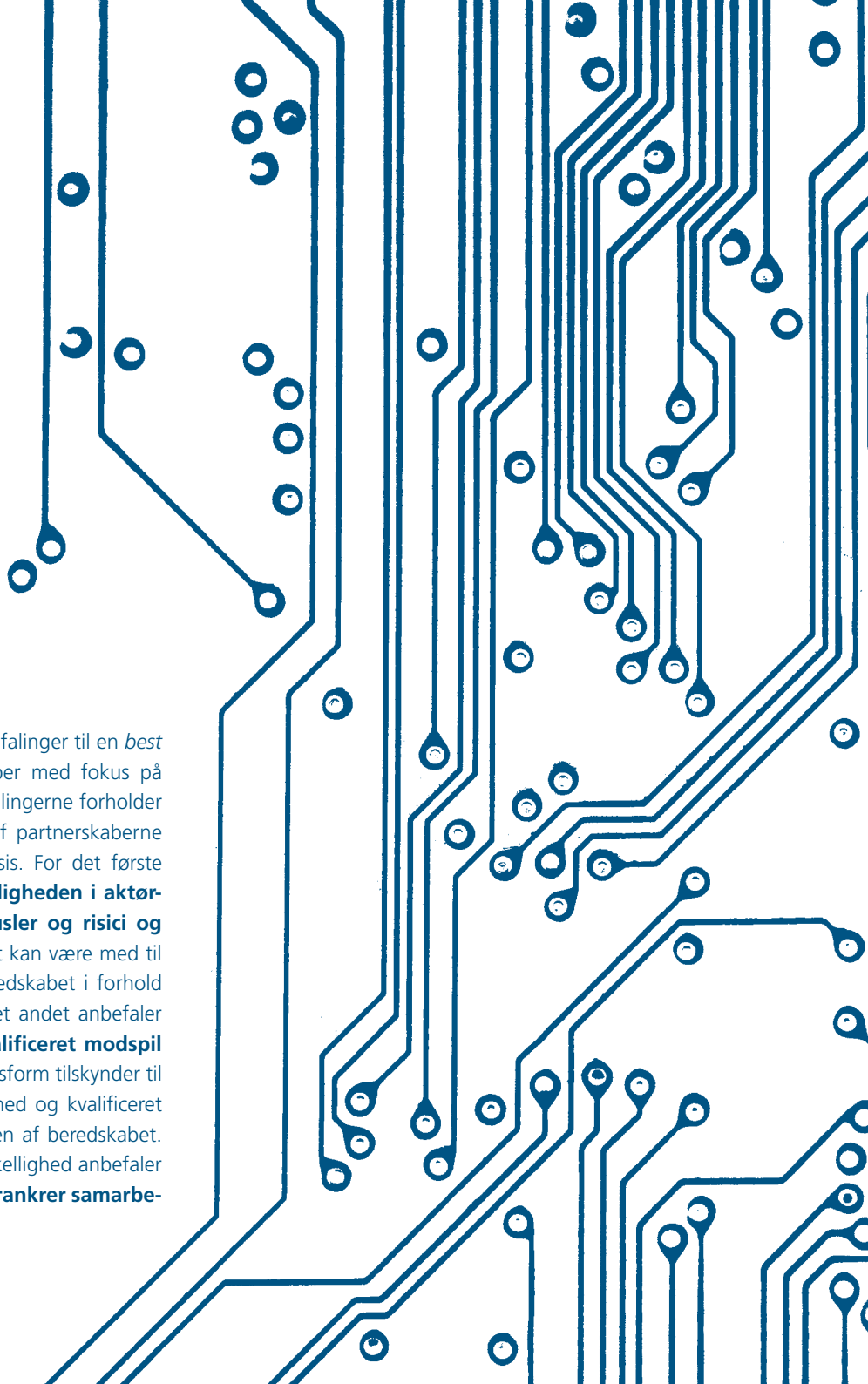
Publication date:
2016

INSTITUT FOR STATSKUNDSKAB
KØBENHAVNS UNIVERSITET

Samarbejde bygget på forskellighed:

Anbefalinger til offentlig-privat samarbejde om IKT-sikkerhed

Kristoffer Kjærgaard Christensen og Karen Lund Petersen · CAST og NordSTEVA



Resume

I dette policy brief fremlægger vi tre anbefalinger til en *best practice* for offentlig-private partnerskaber med fokus på IKT-relateret sikkerhed i Danmark. Anbefalingerne forholder sig både til den praktiske udformning af partnerskaberne og til sikringen af en demokratisk praksis. For det første anbefaler vi, at man **accepterer forskelligheden i aktørernes forståelse af IKT-relaterede trusler og risici og bruger den konstruktivt**. Denne accept kan være med til at sikre nytænkning og innovation i beredskabet i forhold til det omskiftelige trusselsbillede. For det andet anbefaler vi en samarbejdsform med fokus på **kvalificeret modspil og repræsentativitet**. Denne samarbejdsform tilskynder til en kommunikation baseret på forskellighed og kvalificeret modspil og bidrager derved til udviklingen af beredskabet. For at understøtte mulighederne for forskellighed anbefaler vi for det tredje, at man organisatorisk **forankrer samarbejdet ét sted og undgår silotænkning**.

Indledning

I takt med digitaliseringen af samfundet og udbredelsen af informations- og kommunikationsteknologi (IKT) er IKT-relaterede sikkerhedsspørgsmål blevet genstand for stadig større bevågenhed. De sikkerhedsmæssige udfordringer relateret til IKT er mangeartede, komplekse og omskiftelige, og det er den gængse opfattelse, at de ikke kan klares af staten alene. Størstedelen af IKT-infrastrukturen ejes og drives af private virksomheder, og inddragelse af den private sektor er således central for håndteringen af disse udfordringer. Denne inddragelse skal sikre ikke alene hurtig og effektiv implementering af sikkerhedstiltag, men også fleksibilitet og åbenhed over for et stadigt mere omskifteligt og diffust trusselsbillede. På denne baggrund efterspørges der i stigende grad offentlig-privat partnerskaber med fokus på IKT-relaterede sikkerhedsspørgsmål.

Dette gør sig også gældende i Danmark. Trods den generelle efterspørgsel efter sådanne offentlig-private partnerskaber er der dog stadig en række udfordringer i forhold til at opnå et stærkt og velfungerende offentlig-privat samarbejde om IKT-relaterede sikkerhedsspørgsmål i Danmark. I policy briefet *Udfordringer ved offentlig-privat samarbejde om IKT-relateret sikkerhed: Trusler, kommunikation, nytte* pegede vi på tre væsentlige udfordringer og dilemmaer:

- **Trusselsbillede**: De offentlige og private parter ser forskelligt på truslerne og risiciene relateret til IKT og har forskellige bud på, hvordan de bedst imødekommes; om fokus skal være på den truende part (fx andre stater eller kriminelle) eller på de værdier, vi ønsker at beskytte (organisationers og institutioners sårbarheder).

- **Kommunikationsformer**: Der efterspørges mere dialog og vidensdeling mellem offentlige institutioner og private virksomheder og dermed et opgør med den form for envejskommunikation, som tidligere har præget samarbejdet.

- **Nytte**: Det er uklart, hvad formålet af samarbejdet skal være. Her er der igen meget forskellige forståelser; skal det handle om operativ erfaring; om strategiske beslutninger i forhold til nationens sikkerhed; eller er det viden om ny lovgivning og andre formelle tiltag, som samarbejdet skal baseres på? Alt dette giver desuden usikkerhed i forhold til både ansvar og forankring af samarbejdet.

Med udgangspunkt i disse udfordringer fremlægger vi i dette policy brief tre anbefalinger til en best practice for offentlig-private partnerskaber med fokus på IKT-relateret sikkerhed i Danmark. Anbefalingerne forholder sig både til den praktiske udformning af samarbejdet og til sikringen af en demokratisk praksis, når private virksomheder inddrages i det sikkerhedspolitiske arbejde, som tidligere var statens eksklusive domæne.

Accepter forskelligheden og brug den konstruktivt!

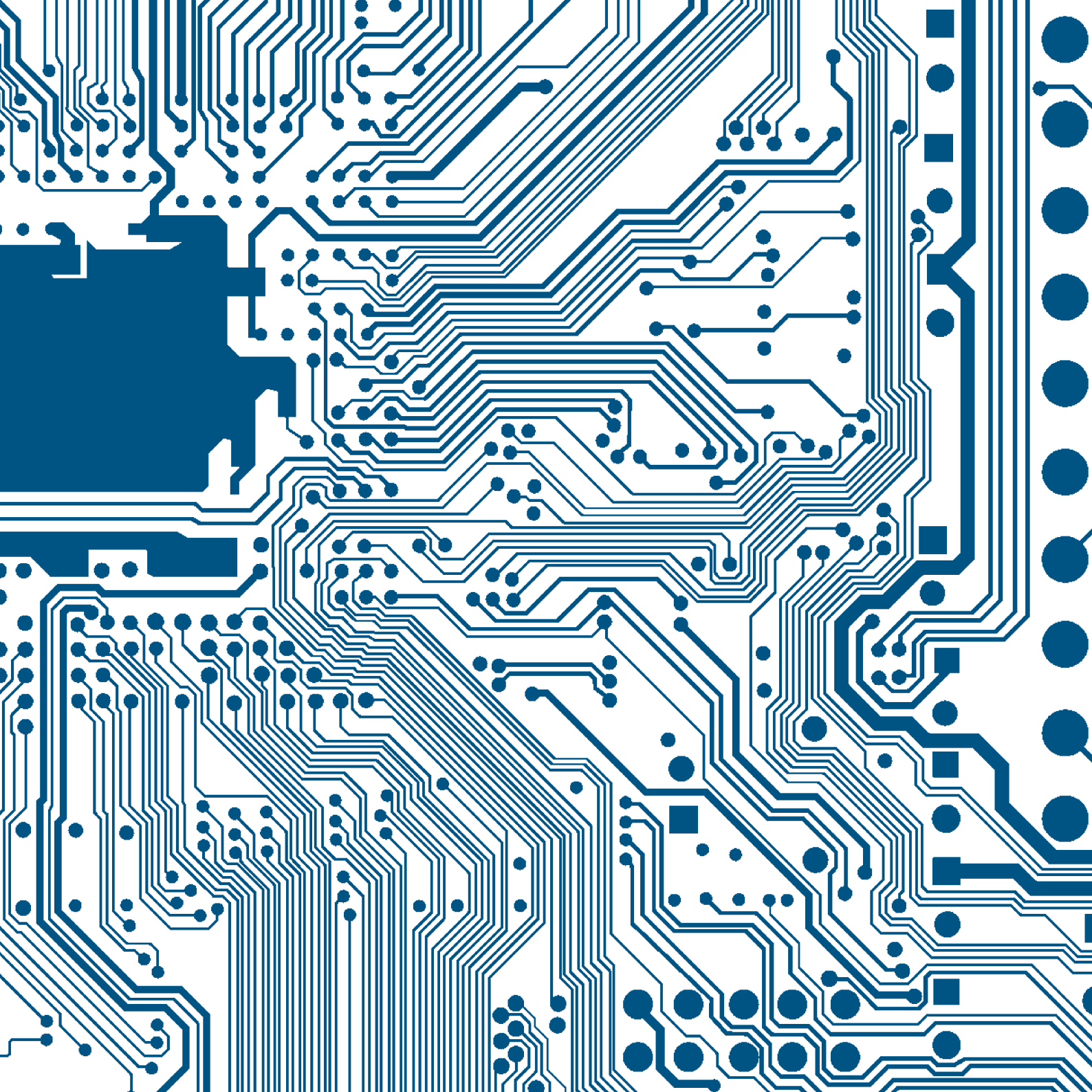
Trusselsbilledet relateret til IKT er præget af mangfoldighed, kompleksitet og omskiftelighed. Vores undersøgelse viser, at offentlige myndigheder og private virksomheder i Danmark fokuserer på og prioriterer forskellige trusler relateret til IKT. Hvor de statslige institutioner på klassisk sikkerhedspolitisk vis søger at *identificere motivet og bekæmpe aktøren* bag truslerne (dvs. fastslå om truslen stammer fra fx andre stater eller kriminelle), fokuserer virksomhederne i langt hører grad på at *identificere og beskytte deres sårbarheder* og dermed deres kerneydelser/produkter. Disse divergerende prioriteringer og forståelser af truslens karakter er en central udfordring i forhold til at fostre offentlig-privat samarbejde. Udfordringen består dog ikke i divergensen som sådan, men snarere i en manglende erkendelse af denne forskellighed. Et samarbejde baseret på en ens opfattelse af problemet er hverken realistisk eller frugtbart: Det er urealistisk, fordi myndighederne og virksomhederne har forskellige hensyn at tage (groft sagt forskellen mellem hensynet til henholdsvis national sikkerhed og økonomisk vækst). Det er ufrugtbart, fordi behovet for konsensus bidrager til at gøre samarbejdet relativt trægt og ufleksibelt i forhold til at udpege og håndtere nye trusler og risici. Løsningen er derfor ikke at efterstræbe ensretning af trusselsbilledet aktørerne imellem, men at skabe et rum for vidensdeling baseret på forskellighed i de prioriteringer, som må laves. Kort sagt bør man acceptere forskelligheden som præmis og vende den til noget konstruktivt.

En erkendelse af forskelligheden vil opfylde to vigtige funktioner: Den vil skabe større relevans for aktørerne og bidrage til at åbne op for innovation og nytænkning i forhold til IKT-relateret sikkerhed i Danmark. Den større relevans skabes ved at erkende, at et samarbejde baseret på konsensus vil være begrænsende, i og med at der kun samarbejdes om de trusler og risici, man kan blive enig om er vigtige. Accepten af forskelligheden gør derimod, at samarbejdet potentielt kan udbredes til alle de trusler, som de enkelte deltagere finder relevante. Her kan forskelligheden bruges som en konstruktiv drivkraft, der skaber grobund for reel vidensdeling og konstant udfordring af eget fokus. Dermed sikres løbende tilpasning og styrkelse samt nytænkning og innovation i forhold til beredskabet – både fælles og for den enkelte deltager. Et samarbejde, hvor vidensdeling baseret på forskellige trusselsbilleder er dagsordenen, vil både øge udbyttet af samarbejdet for den enkelte, samtidig med at det bidrager til hele nationens sikkerhed.

Men hvilken viden er mulig at dele? Baseret på undersøgelsen skelnes der mellem tre typer af viden:

1. Efterretningsbaseret viden om konkrete nationale trusler (de statslige tjenester)
2. Operativ viden om systemer til beskyttelse af IKT-infrastruktur (primært virksomheder)
3. Branchespecifik viden: Nye prioriteringer, politikker og lovgivning, der berører sikkerheden (brancheorganisationer, virksomheder og statslige tjenester)

Hvilke af disse videnstyper, der skal deles i samarbejdet, kan ikke defineres på forhånd. Som en del af erkendelsen af forskelligheden og tilpasningen til de skiftende udfordringer må dette nødvendigvis være til løbende debat. I forlængelse af dette spørgsmål om indholdet af den dialog og vidensdeling, som påtænkes, rejser sig yderligere spørgsmål om, hvordan samarbejdet skal organiseres, sammensættes og institutionelt forankres.



Giv plads til kvalificeret modspil og repræsentativitet!

Det nuværende samarbejde mellem myndigheder og virksomheder er præget af, hvad de fleste forstår som envejskommunikation; det er baseret på, at myndighederne informerer virksomhederne om trusler og tendenser, og at virksomhederne handler herpå. Lidt karikeret kan man sige, at der her er tale om en hierarkisk relation mellem myndighederne og virksomhederne, hvor definitions- og prioriteringsretten er placeret hos førstnævnte. Virksomheden anses mest som passiv modtager af denne viden. Denne relation er dog ikke overraskende: Den gentager blot den model, som altid har kendetegnet organisering af national sikkerhedspolitik – en model hvor statslig styring antages at være i alles interesse. I forbindelse med IKT-relateret sikkerhed er problemet dog – som nævnt ovenfor – at staten er dybt afhængig af vidensdeling "den anden vej", da meget IKT infrastruktur ejes af private virksomheder. Derfor er det reelt nødvendigt, at alles behov varetages, og de forskellige prioriteringer anerkendes. Det er da også sådan, som vi påpeger i *Udfordringer ved offentlig-privat samarbejde om IKT-relateret sikkerhed: Trusler, kommunikation, nytte*, at såvel private virksomheder som offentlige myndigheder faktisk efterspørger en mindre hierarkisk form for samarbejde; en form hvori private virksomheder indgår som ligeværdige og definerende partnere i håndteringen af IKT-relaterede sikkerhedsspørgsmål. Der efterspørges kort sagt en samarbejdsform, som baseres på dialog og fælles prioritering og håndtering af de relevante udfordringer – med andre ord en konsensusorienteret model.

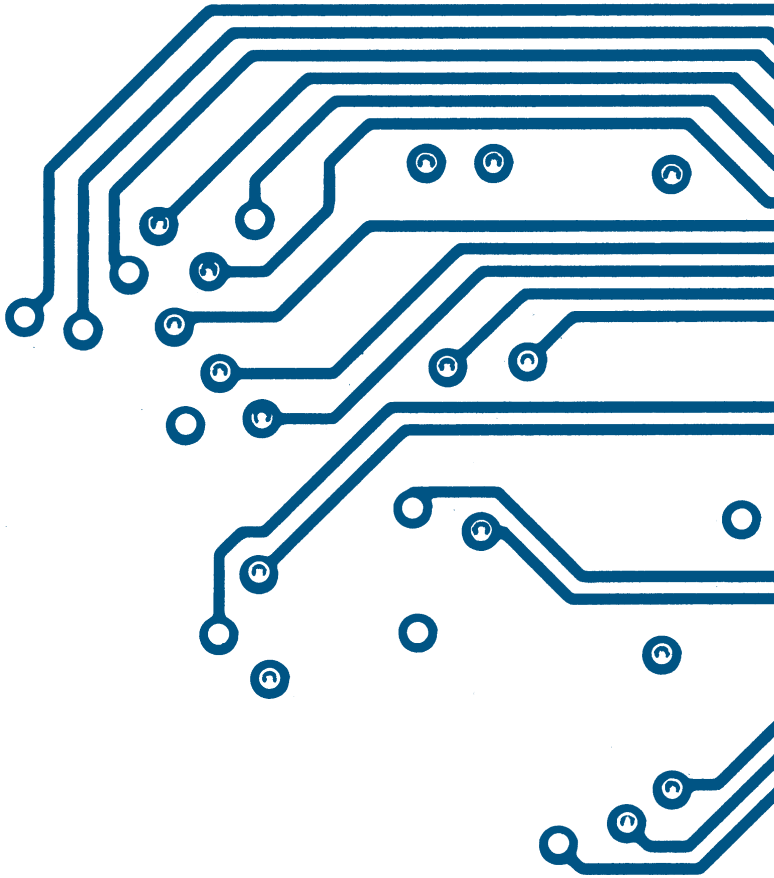
Vi vil dog anbefale en helt tredje samarbejdsform – én som er baseret på kvalificeret modspil og repræsentativitet. Tanken bag denne samarbejdsform er at skabe et rum, hvor det er legitimt at udfordre hinandens trussels- og vidensforståelser. Formålet er ikke at opnå konsensus om fælles mål og midler, men snarere at få repræsenteret så mange forskellige tilgange til og forståelser af sikkerhed som muligt. Der er tale om en samarbejdsform, hvor uenighed og repræsentation tilskyndes og ses som et gode. Derved bringes forskelligheden i spil, og mulighederne for nytænkning

FIGUR 1: **SAMARBEJDSFORMER**

	Envejskommunikation	**Dialog**	**Kvalificeret modspil**
Relation	Hierarkisk (ekspertorienteret)	Ligeværdig (fælles skabelse af ekspertise)	Ligeværdig (fælles skabelse af ekspertise)
Formål	Informationsdeling (sender/modtager-relation)	Konsensus (enighed)	Repræsentativitet (kritisk modstand)

og innovation i arbejdet med IKT-relateret sikkerhed bliver understøttet. Desuden bidrager denne samarbejdsform med sit fokus på forskellighed og kritisk modstand til en demokratisk dialog. En demokratisk dialog er særligt vigtig i forhold til IKT-relaterede sikkerhedsspørgsmål, hvor det diffuse, omskiftelige og potentielt altomsluttende trusselsbillede hurtigt kunne blive til et sikkerhedspolitisk carte blanche. En samarbejdsform baseret på kritisk modstand og repræsentativitet kan altså både bidrage til et velfungerende og demokratisk legitimt offentlig-privat samarbejde.

For at denne form for samarbejde kan fungere i praksis, er fortrolighed dog et væsentligt element. Fortroligheden er her baseret på, at de enkelte partnere kan sige deres mening og fortælle om deres oplevelser uden at frygte misbrug af informationerne eller at blive udstillet som (u)ansvarlig. For at skabe sådan et fortroligt rum kan man med fordele skele til *Chatham House Rules* og de n*on disclosure agreements*, som kendes fra private sikkerhedsnetværk. Bagsiden ved dette princip om fortrolighed og hemmeligholdelse er naturligvis, at det oftest står i vejen for gennemsigtighed og muligheden for offentlig debat om sikkerhedspolitikken. Derfor er det også meget vigtigt, at man ved etableringen af disse partnerskaber sikrer åbenhed og repræsentativitet i udvælgelsen og sammensætningen af partnerskabernes deltagere. Dette kan fx ske gennem offentligt tilgængelige oversigter over deltagerne i partnerskaberne. Ydermere kunne man med fordel udgive en årlig rapport om partnerskabets resultater, hvor informationerne ikke kan spores tilbage de enkelte deltagere, men derimod giver offentligheden indsigt i arbejdet og bidrager til at højne dets eksterne legitimitet.



Forankr kontakten ét sted og undgå silotænkning!

En væsentlig forudsætning for at bringe forskelligheden i spil og sikre kvalificeret modspil og repræsentativitet er at undgå silotænkning. Hidtil har myndighedernes organisering i forhold til IKT-relaterede trusler og risici – ligesom resten af det danske beredskab – fulgt sektoransvarsprincippet og inddelt trusselsbilledet i henhold til de enkelte myndigheders respektive ansvarsområder. Blandt de private virksomheder findes der også mere sektorspecifikke former for samarbejde i visse brancher, men der er dog generelt en bredere tilgang til trusselsbilledet. Udfordringen ved den sektor- og/eller myndighedsbaserede inddeling er, at man risikerer, at noget falder mellem stolene, fordi det ikke umiddelbart er klart, hvor det hører hjemme – dvs. om den pågældende viden skal deles med fx Center for Cybersikkerhed eller med NC3. Man risikerer dermed, at relevant viden slet ikke bliver delt.

Derfor anbefaler vi et organisatorisk setup med én enhed som kontaktpunkt mellem myndigheder og virksomheder. Den pågældende enhed ville således være ansvarlig for at fortolke og fordele de relevante informationer i forhold til henholdsvis efterretning (Center for Cybersikkerhed) og efterforskning (NC3). Ved at gøre op med behovet for en forudgående fortolkning og kategorisering af deltagernes viden fjernes en af de nuværende barrierer for vidensdeling. Det er dermed et vigtigt skridt i retning af at få bragt så meget som muligt forskellig viden i spil i bestræbelserne på at skabe et mere robust og fleksibelt beredskab.

Anbefalingen af én koordinerende enhed er inspireret af modellen for Center for Terroranalyse. Ved at samle funktionen ét sted sikres også en bedre koordination af indsatsen og en bedre udnyttelse af ressourcerne på IKT-området. Den koordinerende funktion kunne med fordel samles hos Center for Cybersikkerheds nyetablerede trusselsvurderingsenhed, således at samarbejdet mellem myndigheder og virksomheder kan bidrage til relevante og opdaterede trusselsvurderinger og –analyser. Placeringen af den koordinerende funktion i trusselsvurderingsenheden er ikke ensbetydende med, at hverken CfCS eller staten som sådan ensidigt skal definere samarbejdet; man kunne sagtens forestille sig fx et roterende formandskab for enheden eller lignende. Samarbejdet må dog nødvendigvis forankres i staten, da myndighederne ikke kan legitimere deltagelse i sikkerhedspolitiske partnerskaber, som er forankret i den private sektor og dermed uden for den demokratiske kontrol med sikkerhedspolitikken.

Rev C
593-1104-A LW
R. SPKR
L. SPKR

Konklusion

Uenighed gør stærk. Det er i korte træk hovedbudskabet i dette policy brief. Her har vi peget på tre centrale anbefalinger til en best practice for offentlig-private partnerskaber i forbindelse med IKT-relateret sikkerhed:

- Acceptér forskelligheden og brug den konstruktivt!
- Giv plads til kvalificeret modspil og repræsentativitet!
- Forankr kontakten ét sted og undgå silotænkning!

Formålet med disse anbefalinger er at skabe basis for en samarbejdsform, der sikrer en konstruktiv og kontinuerlig proces, snarere end at definere et endegyldigt mål for samarbejdet. Partnerskabernes omfang og fokus skal i stedet defineres løbende, men i udgangspunktet fokusere på såvel strategiske og efterretningsmæssige trusler som på operative og branchespecifikke muligheder og udfordringer.

Ved at bringe forskelligheden i spil og give plads til kvalificeret modspil og repræsentativitet bidrager anbefalingerne til, at beredskabet konstant udfordres og videreudvikles – til både fælles gavn og til gavn for den enkelte myndighed og virksomhed. Anbefalingerne er dermed med til at sikre et interessefælleskab og skabe relevans og merværdi for deltagerne, som får mulighed for påvirke sikkerhedspolitikken på IKT-området og gøre opmærksom på de trusler og risici, som er relevante for dem.

Ligeledes bidrager anbefalingerne til at sikre demokratisk legitime partnerskaber. Ved at sikre repræsentativitet og kvalificeret modspil lægges der et nødvendigt bånd på sikkerhedspolitikkens privilegium. Den demokratiske kontrol skal dog ikke baseres på fuldstændig transparens om partnerskabernes indhold. Tværtimod fordrer den anbefalede form for samarbejde, at viden og forskellige synspunkter kan deles i fortrolighed. Den demokratiske kontrol bør derimod baseres på repræsentativitet og gennemsigtighed omkring deltagerne i partnerskaberne. Befolkningen skal have indsigt i udvælgelsen af de organisationer og virksomheder, som inddrages i arbejdet, og dermed viden om, hvem det er med til at definere IKT-sikkerheden i Danmark.

Januar 2016

Ph.d.-stipendiat Kristoffer Kjærgaard Christensen (kk@ifs.ku.dk)
Lektor Karen Lund Petersen (klp@ifs.ku.dk)

CAST og NordSTEVA